ABSTRACT

Apparatus and method for generating a key stream is disclosed. In one embodiment, a cryptographic function is applied on input values selected from a first array of values to generate output values. Mask values are then selected from a second array of values and combined with the output values to generate a key stream block for the key stream. The first and second arrays are finite and may be implemented by a linear feedback shift register.